Mile High Dice

Cybersecurity Seminar & Tabletop Exercise

November 10, 2016

Welcome

GAY PAGE
Colorado Federal Executive Board
Executive Director

JIM GRAY
Department of Justice | Bureau of Prisons | National Corrections Academy
Director

FRED EIDSON
Department of Commerce | Economic Development Administration
Administrative Director and CFEB Chair

NANCY DRAGANI
Department of Homeland Security | FEMA Region VIII
Regional Administrator (a)

Thank You

BOP	Jim Gray, Director
FEMA	Nancy Dragani, Reg Administrator (a)
	Mike Brinkman
	Mary Beth Vasco
DHS NCEPP	Aldo Vega
	Jim Harris
	Gary Benedict
	Ben Coyle
CFEB	Fred Eidson, Chair
	Gay Page
	Jeff Conn
	Donna Vallejos, GSA
	Jackie Mead, ONRR
	Sheila Perry, ONRR
STATE OF CO	Jory Maes
	Fran Santagata
DHS NPPD	Joe O'Keefe
	Jamie Richards
	Harley Rinerson
WAPA	Randy Dreiling
	Tiffani DeFore
	Orlando Reyes
CEPP	Pat Williams

Welcome

GAY PAGE
Colorado Federal Executive Board
Executive Director

JIM GRAY
Department of Justice | Bureau of Prisons | National Corrections Academy
Director

FRED EIDSON
Department of Commerce | Economic Development Administration
Administrative Director and CFEB Chair

NANCY DRAGANI
Department of Homeland Security | FEMA Region VIII
Regional Administrator (a)

Purpose

Mile High DICE provides a forum for interagency coordination and improvement of continuity and response plans.

The 2016 theme is cybersecurity, which is the RISC (Regional Interagency Steering Committee) priority this year.

DICE establishes a learning environment for participants to improve their understanding of a cyber incident and examine response/contingency plans to determine their ability to continue their mission essential functions.

Objectives

Develop a common understanding of:

- Cybersecurity threats and vulnerabilities
- Cyber resources available from the government

Identify cyber gaps or vulnerabilities that could disrupt delivery of mission essential functions

Discuss response and recovery of mission essential functions following a cyber event

Deliver sample tools that will assist in the development of a cyber annex in the organization's plan(s).

Agenda

7:30 am	Registration
8:30	Welcome / Opening Remarks
9:30	Scenario 1 | Ransomware
10:30	*BREAK*
10:50	Scenario 2 | Watering Hole
11:50	*LUNCH / On Your Own*
1:10	Scenario 3 | Cyber-Induced Power Outage
2:10	*BREAK*
2:30	Scenario 4 | Insider Threat
3:30	Wrap Up
3:45	Adjourn

Introductions

TABLE INTRODUCTIONS

- Name
- Agency
- Title

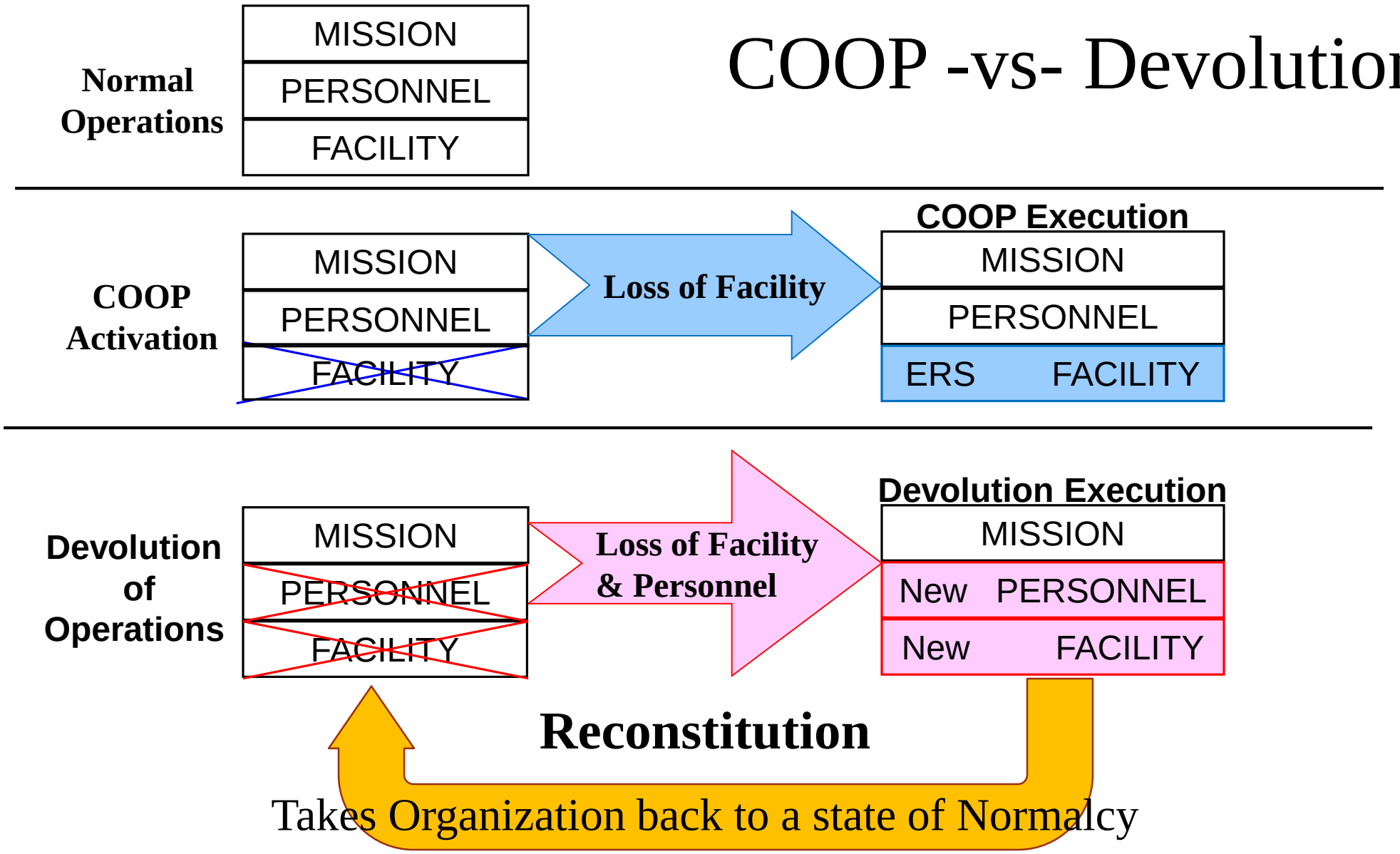
SELECT A FACILITATOR

SELECT A SCRIBE

Want to change tables? Now is the time.

COOP in 90 Seconds

COOP -vs- Devolution



Mile High DICE Cybersecurity Tabletop Exercise

November 10, 2016

Exercise Facilitator

Jim Harris

Department of Homeland Security - National Cybersecurity & Communications Integration Center (NCCIC) - National Cyber Exercise & Planning Program (NCEPP)

Background

- Engineer/scientist for IBM in the mid-nineties
- Joined FBI after 9/11, served in Cyber Division, final assignment as Assistant Section Chief of Counterterrorism Internet Operations.
- Consultant for public and private sector companies for planning and preparing for cyber incidents since 2013.

Homeland Security

Exercise Structure

- This will be a facilitated, discussion-based exercise
- Players will participate in the following four vignettes:
  - Scenario Vignette #1: Ransomware Attack
  - Scenario Vignette #2: Watering Hole Attack
  - Scenario Vignette #3: Cyber-Induced Power Outage
  - Scenario Vignette #4: Insider Threat
- This exercise will conclude with a brief Hotwash.

Participant Roles and Responsibilities

Players	Respond to situation presented based on current plans, policies, and procedures
Scribes	Observe and document player discussions
Facilitator	Provide situation updates and moderate discussions

Homeland Security

Guidelines – Facilitated Discussion

- This is an open, low-stress environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans, capabilities (i.e., you may use only existing assets) and insights derived from your training.
- This discussion is not precedent setting and may not reflect your organization's final position on a given issue. This is an opportunity to discuss and present multiple options and possible solutions.
- Assume cooperation and support from other responders and agencies.

Guidelines (cont.)

- The exercise is conducted in a no-fault learning environment.
- There is no “hidden agenda” nor are there any trick questions.
- The exercise scenario is plausible, and events occur as they are presented.
- All players receive information at the same time.
- The scenario is not derived from current intelligence.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, detection, protection, mitigation, response, and recovery efforts.
- Avoid using acronyms.

Cyber TTX
Facilitated Discussion

Homeland Security

Scenario Vignette 1: Ransomware Attack

Homeland Security

State of the World

- With the advent of the digital age and our reliance on electronics ranging from mobile devices to Bluetooth-enabled vehicles, we have gained several benefits such as efficiency and convenience.

- Taking advantage of weak cybersecurity policies and measures, malicious actors navigate these weaknesses with relative ease, capturing valuable information. The attacks can be in the form of brute force attacks, distributed denial of service (DDoS) attacks, phishing, Trojans, and others.

- Ransomware has provided a lucrative means to attack all types of sectors to include medical and education sectors. These particular attacks have increased throughout 2016.

Digging for Gold – Day 1

- Law enforcement, IT officials, and other security staff review their respective daily/weekly intelligence and information products from various government and private sector sources, noting the rise in ransomware occurrences.

- The HR department in an organization receives an email from a prospective employee requesting advice on applying for a job. The email contains a resume in an attached PDF. The prospective employee provides information about the attachment and a cover letter describing why he is the perfect candidate for a particular job opening.

- Several recruiters (or hiring managers) open the attachment to look at the application and some reply offering advice to the prospective employee.

Digging for Gold – Day 3

- A few days later, employees are unable to log into their systems and a screen displaying a message, similar to the one below, appears on their screens. The message states all files are encrypted and 100 Bitcoins are required to be paid to unencrypt the files.

Homeland Security

Discussion Questions

- What actions do you initially take?
- Describe your current cybersecurity-related policies. What protocols/policies are in place for downloading files?
- Does your organization provide basic cybersecurity awareness training to all employees (including managers and senior executives)? How often is training provided?
- Is training provided to new employees before they access your information systems?
- What other resources are available to assist your organization in a cyber incident?
- Do you pay the ransom? Why or why not?

Homeland Security

Break

Reconvene in 20 Minutes

Scenario Vignette 2: Watering Hole Attack

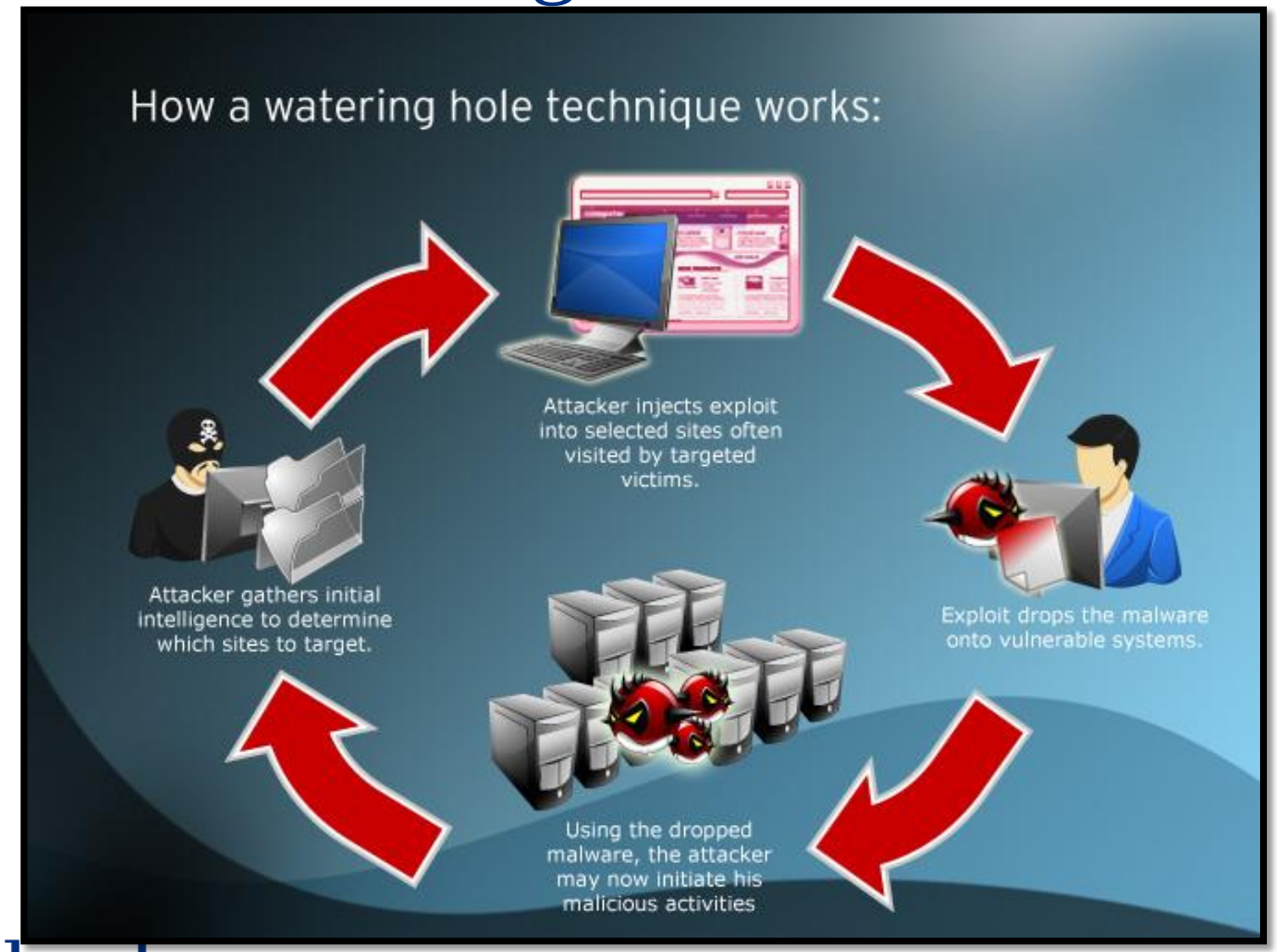
Homeland Security

Quench the Thirst

- Organizations that have intellectual property or are perceived to have something of value often become targets for cyber espionage or theft. One technique malicious actors use is watering holes.
- The main purpose behind watering holes is to steal information or conduct espionage activities. Hackers' motivations are to steal intellectual property, personal information, or gain access to sensitive computer systems.
- Watering hole attacks are very difficult to detect.

Homeland Security

Watering Hole Attack



Homeland Security

Thirsty?

- D-day – Employees receive an email from the training division. The email states each employee must complete mandatory training by the end of the week. Contained within the email is a link to the trusted training website.
  - The subject of the training: Keeping Your Information Safe During the Holidays
- A malicious actor has discovered that employees of the target company are visiting the trusted training website and plants malware in the website.
- As employees access the trusted website the target company systems become infected.

Thirsty? (cont.)

- D +1 – Employees who have attempted to email the completed training certificate report having trouble with the link. They report their systems are hung up. Not all employees are having the same issue though.

- IT personnel troubleshoots the issue and realize one of the browsers is incompatible with the training website. The employees are then instructed to use a different browser to complete the training.

- D +2 – Employees who successfully completed training report they are unable to log into their organization-specific application. The error message states, “You are already logged in at another location. Please log off from that location first.”

Thirsty? (cont.)

- D +3 – While investigating the log on error, IT personnel notice the individual's credentials are logged into the application from an overseas Internet Protocol address and a large amount of data has been exfiltrated.

- D +4 – Analysis is conducted on all machines that exhibit the error message. IT personnel discover sophisticated malware was uploaded from the trusted training website.

Discussion Questions

- Who in your organization would respond to this incident and how?
- What are their roles and responsibilities?
- What resources and capabilities are required to respond to this incident?
- Are essential personnel trained to respond to this scenario?
- What actions would your organization take based on this information?
- Does your organization have policies and procedures for sharing threat information?

Homeland Security

Lunch

Reconvene at 1:10 pm

Lunch

Reconvene at 1:10 pm

Scenario Vignette 3:
Cyber-Induced Power Outage

Homeland Security

Got Power?

- Many organizations outsource security monitoring of Industrial Control System (ICS) /Supervisory Control And Data Acquisition (SCADA) systems to a third-party vendor in order to save on manpower.
- These third-party vendors often remotely control key systems and provide updates to those systems when needed.
- Sometimes a bad update is pushed, creating a vulnerability and an opportunity for malicious actors to upload malware.
  - This malware may sit on the network just watching (sniffing) the traffic, collecting information on various systems.
  - Once a critical system is identified, a malicious actor conducts a test to ascertain the malware's effectiveness. A successful test could lead to a full scale cyber attack, resulting in rolling brown outs or a black out.

Got Power? (cont.)

- A third-party vendor provides continuous monitoring of ICS and SCADA systems, capable of remotely controlling key systems.
- D-1: The vendor notices there is a new update for printers on the operational system and proceeds with installation.
- D+2: Network personnel notice one of the operational printers is attempting to contact an unknown IP address.
- D+4: The organization experiences a short power outage. Investigation doesn't find anything unusual.

Got Power? (cont.)

- D+5: News reports state a blizzard is forecasted for the area.

- D+7: During the night, third party vendors monitoring the ICS and SCADA systems notice an increasing imbalance between reactive and real power. As the imbalance increases, rolling brown outs begin to affect the region. As the imbalance continues to increase, a black out occurs leaving thousands without power.

- D+8: IT personnel and emergency crews attempt to get the power restored. Investigation into the system does not yield any clues to the cause of the power outage.

Got Power? (cont.)

- D+9: The blizzard impedes efforts to restore power and many blame the snow for the power outage. Various organizations begin to activate their COOP plans.

- D+10 (AM): As crews work around the clock, IT personnel uncover a series of false commands that were issued to the operational network which caused the imbalance.

- D+10 (PM): IT personnel repair the affected system and the power is restored.

- D+15: Further investigation reveals that Dark Energy 3 was installed via the update to the printer that was connected to the operational network.

Discussion Questions

- What are your organization's essential functions and how could they be impacted by a cyber attack?
- What are the information sharing processes for both internal and external stakeholders during a power outage?
- Do you have defined cybersecurity incident escalation criteria, notifications, activations and/or courses of action?
- If your organization is unable to manage the incident internally, what processes are in place to request and manage additional resources?
- What other cyber-related communications has occurred or is required (e.g. public information, reporting mandates, etc.)?

Homeland Security

Break

Reconvene in 20 Minutes

Scenario Vignette 4
Insider Threat

Homeland Security

The Usual Suspects

- Organizations, concerned with hackers attempting to get into their networks, are beginning to look more closely at insider threats, both malicious and unintentional, which can have serious repercussions.

- The biggest impact of an insider breach experienced by some organizations has been damage to brand or reputation and, to a lesser degree, intellectual property loss or financial loss.

- Insider threats continue to be a serious problem, mitigation programs can help organizations strengthen their position against internal threats by providing early detection of threats and a quick response.

The Usual Suspects (cont.)

- Insider threats with malicious intent have different motivations, such as money, pride/ego, ideology, or other reasons.

- Tools that these malicious actors might use could include downloadable malicious files, corrupted USBs/files/websites, or a device that acts as a password sniffer similar to the below example:

Homeland Security

The Usual Suspects (cont.)

- D-day: Employees arrive at their workstations and begin to work on their respective tasks. Nearly all employees bring their personal phones to work and charge them while at work. Phone chargers are everywhere. A disgruntled employee plugs his phone charger into an outlet near several employees who are working on a sensitive project.

- D+1: Some employees notice their files are missing and not organized. Help desk personnel are able to locate some files but not all.

- D+2: Several employees receive notifications from their banks about suspicious account activity. Additionally, the organization receives an alert that details of a sensitive project have been discovered on the dark web and the details of the project is for sale.

The Usual Suspects (cont.)

- D+5: Employees continue to report missing or corrupted files, leading IT personnel to investigate the issue.
- D+7: Upon further investigation, IT personnel discover the employees were logged on in nearly sequential times throughout the past five days. Log activity shows several amounts of data had been transferred to an outside IP address.
- D+8: The disgruntled employee quits work.
- D+8: Law enforcement is contacted and subsequently arrests the wayward coworker, confiscating his computer and other electronic devices.

Discussion Questions

- What are your highest-priority actions when a cyber attack occurs?
- How are actions coordinated across departments/agencies?
- Who (e.g. agency, organization, etc.) is responsible for the big picture (i.e. collating information across multiple reports and sources)?
- When would you engage with local law enforcement?
- Describe your cyber threat information sharing mechanisms, products, and other considerations internal and external to your organization?
- Are processes in place for evidence retention, to aid in potential prosecution?

Homeland Security

Exercise Hot Wash Discussion
Closing Remarks

Homeland Security

Points of Contact

For questions about the DHS National Cyber Exercise and Planning Program (NCEPP), please contact:

CEP@hq.dhs.gov

(703) 235-5641

Homeland Security

RESOURCES

www.colorado.feb.gov

COOP RESOURCES

http://www.fema.gov/continuity-operations

BUSINESS CONTINUITY PLANNING SUITE

https://www.ready.gov/business-continuity-planning-suite

Closing Remarks

Please turn in your Feedback Forms

Thank you!